and, establish a secure connection to the wireless

communication apparatus.

A1 cnceld.

4. (Amended) A method according to claim 1, [2 or 3,] and comprising a step of providing said separate unit in a smart card.

A2

7. (Amended) Wireless communication apparatus according to claim 5 [or 6] wherein the master secret code is stored on the separate unit.

---

9. (Amended) Wireless communication apparatus according to [any one of claims] claim 5 [to 8] wherein the master secret code is generated on the separate unit.

A3

10. (Amended) Wireless communication apparatus according to [any one of claims] claim 5 [to 9] wherein the signature is generated on the separate unit.

11. (Amended) Wireless communication apparatus according to claim [any one of claims] 5 [to 10] wherein the separate unit comprises a smart card.

A4 cmt

13. (Amended) A smart card according to claims 11 [or 12].

A4
Cncld.

14.   (Amended) A wireless communication apparatus according to <u>claim</u> [any one of claims] 5 [to 12] without [the] <u>a</u> smart card [of claim 13].

A5

17.   (Amended) A memory card according to claim 15 [or 16], comprising a secure database provided with at least one master secret code and/or at least one signature related to one or more data communication apparatus, in order to re-establish a secure connection to data communication apparatus.

18.   (Amended) A memory card according to claim 15, [16, or 17, is] provided on a smart card.

A6

21.   (Amended) A system according to claim 19, [or 20,] said memory means is a smart card.

Please add new claims 25-45 as follows:

A7
Cont.

--   25.   A method according to claim 2, further comprising a step of re-establishing the connection by transmitting a request from the wireless communication apparatus to the data communication apparatus, said request comprising the calculated signature based on the chosen algorithm, the public key and the stored secret key, and upon reception of the request, the data communication apparatus calculates the master secret code based on the chosen algorithm, the

signature received, and the private key, and, establish a secure connection to the wireless communication apparatus.

26. A method according to claim 2, and comprising a step of providing said separate unit in a smart card.

27. A method according to claim 3, and comprising a step of providing said separate unit in a smart card.

28. Wireless communication apparatus according to claim 6 wherein the master secret code is stored on the separate unit.

29. Wireless communication apparatus according to claim 6 wherein the master secret code is generated on the separate unit.

30. Wireless communication apparatus according to claim 7 wherein the master secret code is generated on the separate unit.

31. Wireless communication apparatus according to claim 8 wherein the master secret code is generated on the separate unit.

32. Wireless communication apparatus according to claim 6 wherein the signature is generated on the separate unit.

33. Wireless communication apparatus according to claim 7 wherein the signature is generated on the separate unit.

34. Wireless communication apparatus according to claim 8 wherein the signature is generated on the separate unit.

35. Wireless communication apparatus according to claim 9 wherein the signature is generated on the separate unit.

36. Wireless communication apparatus according to claim 6 wherein the separate unit comprises a smart card.

37. Wireless communication apparatus according to claim 7 wherein the separate unit comprises a smart card.

38. Wireless communication apparatus according to claim 8 wherein the separate unit comprises a smart card.

39. Wireless communication apparatus according to claim 9 wherein the separate unit comprises a smart card.